

Security Research Co-op at Cygilant

Job Description:

The Service Research Co-op will work with our Security Research, Security Operations and Product Management teams. You will be key contributor to Cygilant's security as a service offering. Learning how to become a technical security advisor to a group of customers, you will engage with customers to help proactively monitor their security and compliance posture. You will interact with and be trained on security monitoring and security analyst capabilities working in our 24x7 Security Operations Centers (SOC). You will learn security best practices for incident detection, incident response, forensic analysis and remediation process.

Responsibilities

- Track incident activity and ensure all information is collected and analyzed to understand the root cause of an anomaly/suspicious behavior, determine the impact and provide remediation guidance. Prepare custom reports and dashboards as needed.
- Participate in regular calls with customers regarding security and compliance posture, discuss tickets and remediation processes
- Identify potential service and product enhancements. Assist in documenting and communicating these to the Product Engineering team
- Develop new alerts to be used in our SIEM platform and scripts to help automate various SOC Team tasks.

Qualifications

- Passionate about cybersecurity, hungry to learn and grow your career in the InfoSec space
- Pursuing a degree in a Computer Science, Computer Engineering or Electrical Engineering degree program
- Knowledge of basic networking: IPV4, IPV6, HTTP, TCP, SSL, UDP, NAT-ing, Routing, Subnets, Ports
- Familiarity with networking and security technologies: firewalls, routers, switches, LANS, IDS/IPS, Endpoint security, Identify and Access management
- Familiarity with basic network security: device logs, vulnerabilities, OS patching
- Expertise in Windows and Linux shell scripting
- Knowledge of either Python/JavaScript/Perl
- Problem solving and the ability to learn new things

About the team

The Cygilant team provides best in class security as a service to Cygilant customers which consist of IT professionals in mid to large enterprises. Our customers look to Cygilant to be an extension of their lean IT team. Through our Service Delivery and Global Security Operations Centers (GSOC), we provide our customers with Enterprise grade cybersecurity protection at a fraction of the cost.